Response to Prebid Queries					
RFP Ref. No.		CPCM-03/2026-27 Date: 09-Apr-2026 GEM Bid No. GEM/2026/B/7427591			
RFP Name		Request for Proposal (RFP) FOR SELECTION OF SERVICE PROVIDER FOR IMPLEMENTATION & SUPPORT FOR SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT) PLATFORM AND MANAGED DETECTION & RESPONSE SERVICES (MDR)			
Sr. No.	Page No.	RFP Clause	Clause Description	Query	StockHolding Remarks
1	General - Asset Inventory			Please provide a comprehensive and updated list of in-scope assets, categorized by device type (e.g., Firewalls, WAFs, Databases, Servers, and Endpoints), including the specific unit counts for each category.	**Clarification:** Details will be shared with the winning bidder.
2	General - Phased Onboarding			Please identify the specific applications and databases designated as "business-critical" that require prioritized onboarding during the initial phase of the SIEM/MDR deployment.	**Clarification:** Details will be shared with the winning bidder.
3	General - Endpoint Security			Kindly provide details regarding the currently deployed EDR/Endpoint security solutions, including the vendor name, software version, total license count, and the respective contract expiration dates.	**Clarification:** Custom built platfrom from ATOS. Other details are not relevant to the RFP.
4	General - SLA Requirements			Please define the mandatory Recovery Time Objective (RTO), Recovery Point Objective (RPO), and Uptime Service Level Agreements (SLAs) required for the SIEM platform, log storage architecture, and MDR services.	**Clarification:** RTO & RPO details are not relevant from the RFP point of view. SLA's including uptime availability are already mentioned in the RFP
5	General - Infrastructure (VM/OS)			Please provide a breakdown of the server estate across DC, DR, and branch offices. Include counts for physical vs. virtual machines, further categorized by Operating System family (Windows, Linux, Unix).	**Clarification:** Details will be shared with the winning bidder.
6	General - Virtualization			Please specify the hypervisors (e.g., VMware, Hyper-V, KVM) and private cloud platforms (e.g., NSX, Exadata) currently in use, including the approximate scale of the deployment.	**Clarification:** Vmware and Oracle Exadata & PCA are the hypervior platforms existing in the environment. Other Details will be shared with the winning bidder.
7	General-Network Topology			To assist in log forwarding design, please share a high-level network diagram illustrating the connectivity between the DC, DR, and branch offices, including WAN/MPLS links and internet breakout points.	**Clarification:** All logs are centrally pushed to log aggregator server. The bidder has to ensure that the logs are ingested in the SIEM platform which shall be hosted at the Vendor's end. Network details are not relevant to be shared from RFP point of view.
8	General- Bandwidth Specs			Please provide the typical and minimum WAN/Internet bandwidth and latency metrics for branch-to-DC/DR connectivity where SIEM collectors will be positioned.	**Clarification:** SIEM collector agrents have to be installed at servers and appliances level. Sufficient bandwith exists to collect the logs to the log aggregator server. User endpoints logs shall be ingested via integration with Crowdstrike (EDR platform provider)
9	General - Storage & Backup			Please detail the current SAN/NAS and backup infrastructure (vendor, capacity, and retention policies). Additionally, clarify if this existing infrastructure is available for SIEM log storage and archival.	**Clarification:** Existing Log Aggregator has enough storage to store the logs and subsequently ingest into SIEM platform
10	General - Cloud Footprint			Please identify the public cloud providers (AWS, Azure, GCP) currently utilized and list the specific workloads or native security services that must be integrated with the SIEM/MDR monitoring scope.	**Clarification:** There is 1 application hosted in GCP and rest are hosted on premise. GCP hosted applications have app servers, db servers and storage bucket.
11	General - Security Stack			Please provide a complete list of deployed security controls (Firewalls, WAF, IPS, VPN, DLP, DDOS, Proxy, NAC, PAM, etc.), including the respective vendors, models, and firmware versions.	**Clarification:** All type of devices are already mentioned in RFP. Further details shall be shared with the winning bidder
12	General - Identity Mgmt.			Please specify the identity systems in use (Active Directory, LDAP, IDM), including the total user count and a description of the domain/forest structure.	**Clarification:** Details will be shared with the winning bidder.

Response to Prebid Queries					
RFP Ref. No.		**CPCM-03/2026-27 Date: 09-Apr-2026 GEM Bid No. GEM/2026/B/7427591**			
RFP Name		**Request for Proposal (RFP) FOR SELECTION OF SERVICE PROVIDER FOR IMPLEMENTATION & SUPPORT FOR SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT) PLATFORM AND MANAGED DETECTION & RESPONSE SERVICES (MDR)**			
Sr. No.	**Page No.**	**RFP Clause**	**Clause Description**	**Query**	**StockHolding Remarks**
13	16	Solution Implementation – Incident Management and Ticketing Tool	f)Inbuilt incident management and ticketing tool to generate tickets for the alert events generated by the SIEM or Separate tool which have capabilities of seamless integration.	The RFP states that the SIEM solution should have an inbuilt incident management and ticketing tool or support seamless integration with a separate ticketing tool, with capability to populate relevant incident details from SIEM alerts into the ticketing system. Kindly clarify: 1. Whether the bidder is expected to provide a new ITSM / ticketing tool as part of the SIEM–MDR solution, or 2. Whether integration with StockHolding's existing ITSM platform is acceptable and preferred. 3. The current ITSM / ticketing tool used by StockHolding.	**Clarification:** As of now, there is no ITSM tool at Stockholding. As and when Stockholding implements ITSM tool, the same should be integrated with SIEM. Till the time Stockholding does not have ITSM tool, the bidder is expected to have an inbuilt ticketing tool.
14	16	Solution Implementation - Point (m)	m) Bidder will also supply all the necessary hardware, software and supporting accessories etc. for integration of the components supplied for CSOC. REC will supply only the Rack space, power and network points.	Bidder to supply hardware for CSOC. Please clarify whether this includes log collectors, storage appliances, and HA components.	**Clarification:** The required infrastructure example VM server will be made available by Stockholding for log collection purpose.
15	16	Solution Implementation - Point (n)	n) The proposed solution shall have storage for managing and storing logs from various devices. Storage should provide minimum 180 days	Storage requirement mentions minimum 180 days. Please clarify whether 180 days refers to hot/online logs only and whether any cold/archive retention (e.g., 1 year / 2 years) is expected.	**Clarification:** Minimum 180 days is required for online. This should be seamless and searchable. Separate ticket request should not be raised by stockholding to get/check the logs. For logs beyond beyond 180 days and upto 2 years searchable option should be available without raising any ticket
16	Page. 23	Development of Connectors for customized applications/ devices	While it is expected that connectors for all the standard applications and devices will be readily available in the collector and Log management devices, connector for mostly inhouse/custom built applications will need to be developed.	Please share the number of in-house application to estimate the number of custom connector that might require	**Clarification:** Existing custom build applications - None Future expected custom build application - Cannot be decided today. To be built as and when required
17	28–29	Payment Terms & SLA – SIEM–MDR Implementation Go-Live (Part A & Part B)	**Terms and Conditions** **A. Payment:** SL | Description | Payment Terms 1 | One-time Implementation of SIEM Platform* | 50% on SIEM – MDR Implementation Go-Live (Part A-600 devices to be on-boarded to the log collector) 50% on Remaining Device On-boarding Go-Live (Part B-600 devices to be on-boarded to the log collector)	The RFP mentions "Part A – 600 devices to be on-boarded to the log collector" and "Part B – 600 devices to be on-boarded to the log collector", which indicates a total baseline of 1200 devices for SIEM–MDR implementation. Kindly confirm whether bidders should consider 1200 devices as the total in-scope device count for sizing, licensing, infrastructure, and commercials. If yes, please provide the detailed device-wise breakup of these 1200 devices across log source categories (e.g., servers, network devices, security devices, applications, databases, endpoints, cloud platforms, etc.) to enable accurate sizing, effort estimation, and commercials.	**Clarification:** 1. Yes. Total devices shall be 1200 2. Device wise breakup shall be shared with the winning bidder
18				Any requirement for onshore presence / dedicated onsite SOC resources at Stockholding for coordination, incident response?	**Clarification:** Onshore presence is not required
19	15	Solution Implementation – EDR/XDR tool		Please confirm whether MSSP is responsible for policy design for EDR/XDR	**Clarification:** No
20	15	Solution Implementation – SOAR tool		Who will be responsible for author, maintain, and own SOAR playbooks/use-cases, is SOAR as well considered or will be considered lateron in scope of work	**Clarification:** No SOAR platform in place and hence not to be considered in the scope of work
21	15 & 44	Solution Implementation – DR/HA for SIEM tool		Please confirm whether MSSP is responsible for building DR - Disaster Recovery or HA - High Availability setup for SIEM implementation, as on page 44 it is mentioned for only logs and not the complete SIEM setup to run on HA/DR if the primary SIEM goes down, as it may impact live monitoring, (The Service Provider is required to maintain the syslog of the devices installed at DC, DR and NDR locations for a period of 180 days). Please elaborate and provide more details on the same.	**Clarification:** Please refer sections pertaining to SLA and Penalty and Deploy the SIEM-MDR Solution accordingly. Bidder has to ensure the SIEM platform is available as per SLA's and take the necessary steps to ensure uptime availability. It is the choice of bidder to have DR or HA or any other model to upkeep the uptime availability

Response to Prebid Queries					
RFP Ref. No.		**CPCM-03/2026-27 Date: 09-Apr-2026 GEM Bid No. GEM/2026/B/7427591**			
RFP Name		**Request for Proposal (RFP) FOR SELECTION OF SERVICE PROVIDER FOR IMPLEMENTATION & SUPPORT FOR SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT) PLATFORM AND MANAGED DETECTION & RESPONSE SERVICES (MDR)**			
Sr. No.	**Page No.**	**RFP Clause**	**Clause Description**	**Query**	**StockHolding Remarks**
22	36	ANNEXURE – 3 – Technical Criteria & Compliance Sl No. 5	The bidder should have minimum three (3) resources certified/ trained on the proposed SIEM solution	Is there any specific years of experienced resources required (for L1, L2, L3, Lead, etc) as only mentioned for "The bidder should have minimum three (3) resources certified/ trained on the proposed SIEM solution".	No change. Prior experience not required.
23	16	Scope of Work (SOW) > Solution Implementation (J)	j) The solution should be able to handle at least 2000 sustainable EPS and scalable to 5000 Peak EPS.	Please share indicative daily ingest volume (GB/day)	**Clarification:** Based on the EPS range mentioned, bidder has to calibrate the Solution as per this requirement
24	17	Log Correlation	Collected Logs should be correlated according to various predefined criteria for generation of alert and identification of the incident. The correlation rules should be predefined and also user configurable. Correlation rules should be customized by the bidder on regular basis to reduce false positives. In any case false negatives will not be permitted. In case of detection of any such incident, correlation rules must be customized immediately to capture such incidents.	"In any case false negatives will not be permitted." - Request to rephrase as "Best-effort reduction of false negatives with continuous tuning; any material misses to be RCA'd with corrective actions and use-case updates within agreed timelines."	**Clarification:** No Change
25	36	ANNEXURE – 3 (2 & 3)	2. Projects for implementation of SIEM and MDR services with at least 1 deployment not less than 2000 EPS (Events per Second) or a minimum integration of 1000 devices with the deployed SIEMMDR solution each during last 05 (five) years in India Note: Bidder to submit the relevant experience only of the SIEM and MDR tool proposed for this RFP. 3.Projects of SIEM and MDR services implementation in BFSI Sector in India during last 05 (five) years in India	If a bidder has experience in implementing and managing SOC operations for global customers, with services delivered from India, will such experience be considered valid for meeting the stated qualification criteria?	No change
26	10	ELIGIBILITY CRITERIA	7. The bidder must have a direct partnership with the supplier of the SIEM tool. One Service Provider can bid only with one OEM as regards SIEM solution is concerned	If the bidder have an MSSP agreement with OEM, can we submit MSSP agreement instead of MAF ?	MAF to be submitted
27	14	Commercial Bid Evaluation	L1 bidder will be selected based on the lowest quote submitted	Request you to consider QCBS model for bid selection.	No change
28	16	Scope of Work (SOW)	i) The SIEM should be able to collect logs from the devices/applications/databases etc. mentioned by StockHolding as per the SOW including the solutions deployed as part of this RFP. It should be able to collect the logs from devices from geographically dispersed locations i.e. DC, DR and branch offices, etc.	We understand that log collectors will be deployed at DC & DR locations only. Also do you need this in HA? We request you to provide VM for log collectors. Please confirm if your brach locations have connectivity with your DC & DR and the same connectivity can be leverage for centralized log collection ?	**Clarification:** Log Collectors in StockHolding enviornment already exists and will be managed by Stockholding. The log collector is a centralized one. Bidder has to ensure that the logs are ingested from the log collector.
29	16	Scope of Work (SOW)	n) The proposed solution shall have storage for managing and storing logs from various devices. Storage should provide minimum 180 days	Does it mean you need 180 days online ? Or we can proposed 90 days online and 90 days offline log storage ? We understand that all collected logs will be stored at MSSP / cloud location for 180 days and not at Stockholding site, please confirm.	**Clarification:** Minimum 180 days is required for online. This should be seamless and searchable. Separate ticket request should not be raised by stockholding to get/check the logs. 180 days online logs should be made available within SIEM platform where it is hosted and not at Stockholdign site.
30	17	Incident Management Tool	Incident Management Tool	What is the total number of users login to be factored for ITSM ? This is critical in licenses and associated commercial.	**Clarification:** 20 user logins should be factored
31	21	Deliverables	Dashboard - Risks, dependencies, milestones, and work progress can be viewed in a single click – anytime and anywhere transparency	What is the total number of users login to be factored for KPI dashboard ? This is critical in licenses and associated commercial.	**Clarification:** 20 user logins should be factored
32	23	Integration of devices in Managed detection and response along with SIEM Services	g) Forensics to identify the origin of threats, mitigation thereof, initiation of measures to prevent recurrence.	Forensic is a separate on-demand service. We understand this will be provided as a sepeated chargeable line item and not included in the MSSP SOC services.	**Clarification:** Detailed Forensics is out of Scope. However, preliminary foresnics is part of the incident management
33	26	Service Level Agreement (SLA) and Penalty	Service Level Agreement (SLA) and Penalty	We propose the maximum pentalty to be capped at 10%	No Change
34	31	Termination Clause	StockHolding reserves right to terminate the contract by giving 90 days prior written notice in advance against any of the following conditions	Please also include a clause for bidder to have the rights to terminate the contract with 90 days prior notice.	No Change

Response to Prebid Queries					
RFP Ref. No.		**CPCM-03/2026-27 Date: 09-Apr-2026 GEM Bid No. GEM/2026/B/7427591**			
RFP Name		**Request for Proposal (RFP) FOR SELECTION OF SERVICE PROVIDER FOR IMPLEMENTATION & SUPPORT FOR SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT) PLATFORM AND MANAGED DETECTION & RESPONSE SERVICES (MDR)**			
Sr. No.	**Page No.**	**RFP Clause**	**Clause Description**	**Query**	**StockHolding Remarks**
35	47	ANNEXURE - 4 - Commercial Price Bid Format	ANNEXURE - 4 - Commercial Price Bid Format	How to we charge if the ingestion volume exceeds 2000 EPS? What happens if the Part A logs reach 2000 EPS ?	**Clarification:** Based on the EPS range mentioned, bidder has to calibrate the Solution as per this requirement
36	13 & 36	Technical Bid Evaluation	4. OEM solution must be positioned in the respective Leader's quadrant/category of the latest IDC MarketScape or Gartner Magic Quadrant, or Forrester Wave reports for proposed SIEM Solution:	We request the removal of the eligibility criterion requiring solutions to be listed in the Leaders quadrant of the Gartner Magic Quadrant for SIEM. This condition unintentionally restricts capable Indian OEMs with proven expertise. As per the Public Procurement (Preference to Make in India) Order, 2017: • Clause 10 discourages eligibility conditions that exclude local suppliers. • Clause 11 prohibits restrictive or discriminatory criteria against domestic manufacturers. Additionally, recent MeitY directives emphasize avoiding non-essential requirements-such as mandatory inclusion in international analyst reports that may disadvantage Indian cybersecurity providers. In alignment with Atmanirbhar Bharat and Make in India initiatives, we request a review and revision of this criterion to ensure fair, inclusive, and policy-compliant participation.	No change This is not a mandatory requirement for participation but a part of technical scoring criteria.
37	9 & 34	ELIGIBILITY CRITERIA	1. The bidder should be a company registered under Indian Companies Act, 1956 or a Partnership Firm registered under Indian Partnership Act, 1932 with experience of SIEM and MDR services implementation and support for the period of 7 years. Copy of Certificate of Incorporation issued by the Registrar of Companies and Self-declaration by the bidder on it Letter Head duly signed by the Authorized Signatory along with supporting documents for SOC related PO on or before RFP Date	The bidder should be a company registered under Indian Companies Act, 1956 or a Partnership Firm registered under Indian Partnership Act, 1932 with experience of SIEM and/**or** MDR services implementation and support for the period of 7 years.	No change
38	9 & 34	ELIGIBILITY CRITERIA	4. The bidder must have executed a minimum of three (03) projects related to SIEM and MDR services in India during the last five (05) years as of the RFP date, with at least one (01) deployment handling not less than 2000 EPS (Events Per Second) or a minimum integration of 1000 devices with the deployed SIEM-MDR solution. Note: Bidder to submit the experience of proposed SIEM and MDR tool only for this RFP.	The bidder must have executed a minimum of three (03) projects related to SIEM and/ or MDR services in India during the last five (05) years as of the RFP date, with at least one (01) deployment handling not less than 2000 EPS (Events Per Second) or a minimum integration of 1000 devices with the deployed SIEM-MDR solution. Note: Bidder to submit the experience of proposed / any OEM SIEM / MDR tool only for this RFP.	No change
39	30	Performance Bank Guarantee (PBG)	Successful Bidder shall, at own expense, deposit with the StockHolding, within Fifteen (15) days on issuance of PO, a Bank Guarantee (BG) for the value of 5% (Five per cent) of the Contract value (including GST) from scheduled commercial banks as per Annexure - 7	As per the latest amendment in GFR 2017 dated 02-02-2022 (Rule 171 of GFR 2017), Performance Security may be obtained in the form of insurance surety bonds, account payee demand draft, banker's cheque, or bank guarantee. Therefore, we request you revise this clause as "Successful Bidder shall, at own expense, deposit with the StockHolding, within Fifteen (15) days on issuance of PO, a Bank Guarantee (BG) or **Insurance surety Bonds** for the value of **3%** (Three per cent) of the Contract value (excluding GST) from scheduled commercial banks.	No change
40	18	Incident Management Tool	f) Solution should be able to integrate with different tools such as SIEM tool, Vulnerability Management tool etc.	Which is the Vulnerability Management (Nessus, tenable etc) tool in use?	**Clarification:** Nessus Tenable is the Incident Management Tool
41	19	Security solutions to be integrated with SIEM Platform	4. Brand Protection and Monitoring Logs, Website Monitoring Service against Defacement	What is the product vendor for Brand Protection solution, where such solution has already been procured or implemented by StockHoldings?	**Clarification:** iZooLogic is the Brand Monitoring Tool

Response to Prebid Queries					
RFP Ref. No.		**CPCM-03/2026-27 Date: 09-Apr-2026 GEM Bid No. GEM/2026/B/7427591**			
RFP Name		**Request for Proposal (RFP) FOR SELECTION OF SERVICE PROVIDER FOR IMPLEMENTATION & SUPPORT FOR SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT) PLATFORM AND MANAGED DETECTION & RESPONSE SERVICES (MDR)**			
Sr. No.	**Page No.**	**RFP Clause**	**Clause Description**	**Query**	**StockHolding Remarks**
42	19	Security solutions to be integrated with SIEM Platform	12. PIM, PAM, CISCO ISE Logs, CISCO ESA logs,	What is the vendor name of PIM/PAM solution in use?	**Clarification:** Arcon PAM solution is currently implemented
43	19 & 20		Security solutions to be integrated with SIEM Platform - WAF Web Application Firewall NAC Network Access Control Perimeter Firewall and Intrusion Prevention System (IPS) Brand Protection and Monitoring Logs, Website Monitoring Service against Defacement Anti-Phishing Service Logs Packet Analysis Database and Compute Server Audit Logs End Point Protection Active Directory Logs Oracle NSG and VMWare NSX Logs Application Delivery Controller (ADC) Logs PIM and PAM CISCO ISE Logs CISCO ESA logs Routers and Switches Proxy Oracle Exadata and PCA VMware Private Cloud	Provide technology wise count of devices in scope and OEM	**Clarification:** Details will be shared with the winning bidder.
44	16	Solution Implementation	h) While, it is expected that connectors for all the standard applications and devices will be readily available with the Service Provider and connector for mostly in-house/custom built applications will need to be developed. Service Provider is be expected to develop connector for the custom built applications specifically developed for StockHolding.	How many custom applications need to be integrated?	**Clarification:** Existing custom build applications - None Future expected custom build application - Cannot be decided today. To be built as and when required
45	16	Solution Implementation	m) Bidder will also supply all the necessary hardware, software and supporting accessories etc. for integration of the components supplied for CSOC. REC will supply only the Rack space, power and network points.	Does bidder have to supply H/W which will be hosted in customer premises for Log Collectors?	**Clarification:** Log Collectors in StockHolding enviornment already exists and will be managed by Stockholding. The log collector is a centralized one. Bidder has to ensure that the logs are ingested from the log collector.
46	16	Solution Implementation	n) The proposed solution shall have storage for managing and storing logs from various devices. Storage should provide minimum 180 days	Can we provide 1 month Online and 5 month Offline log storage? Is it ok for the logs to be maintained in vendor solution or is it required in On Prem?	**Clarification:** Minimum 180 days is required with online storage within SIEM platform. Offline Logs also to be maintained at vendor end
47	21	Logging of Critical Devices	a) The Service Provider is required to maintain the syslog of the devices installed at DC, DR and NDR locations for a period of 180 days.	Can we provide 1 month Online and 5 month Offline log storage? Is it ok for the logs to be maintained in vendor solution or is it required in On Prem?	**Clarification:** Minimum 180 days is required with online storage within SIEM platform. Offline Logs also to be maintained at vendor end
48	21	Support for Managed Detection and Response Services (MDR Services)	The Service Provider is expected to perform thorough log analysis and take necessary action for In-scope devices as well as co-ordinate with **respective internal team members of StockHolding and close the MDR tickets generated in dashboard to ensure compliance**.	Does SHCIL expect Incident Coordination activity - coordination with SHCIL teams to take a ticket to closure?	**Clarification:** Yes
49	29	A. Payment	1. One-time Implementation of SIEM Platform 50% on SIEM – MDR Implementation Go-Live (Part A-600 devices to be on-boarded to the log collector) 50% on Remaining Device On-boarding Go-Live (Part B-600 devices to be on-boarded to the log collector)	We request to modify the clause as below:- 70% on SIEM – MDR Implementation Go-Live (Part A-600 devices to be on-boarded to the log collector) 30% on Remaining Device On-boarding Go-Live (Part B-600 devices to be on-boarded to the log collector)	**Clarification:** No Change

Response to Prebid Queries					
RFP Ref. No.		**CPCM-03/2026-27 Date: 09-Apr-2026 GEM Bid No. GEM/2026/B/7427591**			
RFP Name		**Request for Proposal (RFP) FOR SELECTION OF SERVICE PROVIDER FOR IMPLEMENTATION & SUPPORT FOR SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT) PLATFORM AND MANAGED DETECTION & RESPONSE SERVICES (MDR)**			
Sr. No.	**Page No.**	**RFP Clause**	**Clause Description**	**Query**	**StockHolding Remarks**
50	36	ANNEXURE – 3 – Technical Criteria & Compliance	Technical Criteria 2. Projects for implementation of SIEM and MDR services with at least 1 deployment not less than 2000 EPS (Events per Second) or a minimum integration of 1000 devices with the deployed SIEM-MDR solution each during last 05 (five) years in India Note: Bidder to submit the relevant experience only of the SIEM and MDR tool proposed for this RFP.	We request to modify the clause as below:- Projects for implementation of SIEM and SOC/MDR services with at least 1 deployment not less than 2000 EPS (Events per Second) or a minimum integration of 1000 devices with the deployed SIEM and SOC/MDR solution each during last 07 (seven) years in India Note: Bidder to submit the relevant experience only of the SIEM and SOC/MDR tool.	No Change
51	36	ANNEXURE – 3 – Technical Criteria & Compliance	Technical Criteria 3. Projects of SIEM and MDR services implementation in BFSI Sector in India during last 05 (five) years in India	We request to modify the clause as below:- Projects of SIEM and SOC/MDR services implementation in BFSI Sector in India during last 07 (Seven) years in India	No change
52	36	ANNEXURE – 3 – Technical Criteria & Compliance	Technical Criteria 6. Customer reference for proposed SIEM-MDR Solution during the last 5 years as on RFP date	We request to modify the clause as below:- Customer reference for SIEM and SOC /MDR Solution during the last 5 years as on RFP date	No change
53	34	ANNEXURE - 2 – Eligibility Criteria	4. The bidder must have executed a minimum of three (03) projects related to SIEM and MDR services in India during the last five (05) years as of the RFP date, with at least one (01) deployment handling not less than 2000 EPS (Events Per Second) or a minimum integration of 1000 devices with the deployed SIEM-MDR solution. Note: Bidder to submit the experience of proposed SIEM and MDR tool only for this RFP.	We request to modify the clause as below:- The bidder must have executed a minimum of three (03) projects related to SIEM and SOC/MDR services in India during the last five (07) years as of the RFP date, with at least one (01) deployment handling not less than 2000 EPS (Events Per Second) or a minimum integration of 1000 devices with the deployed SIEM and SOC/MDR solution . Note: Bidder to submit the experience of SIEM and SOC/MDR tool only for this RFP.	No change
54	9	ANNEXURE - 2 – Eligibility Criteria	7. The bidder must have a direct partnership with the supplier of the SIEM tool. One Service Provider can bid only with one OEM as regards SIEM solution is concerned	**Request for Modification:** The bidder must have a direct partnership with the supplier of the SIEM tool. ~~One Service Provider can bid only with one OEM as regards SIEM solution is concerned~~ **Justification:** Most qualified bidders maintain partnerships with multiple Gartner Leader SIEM OEMs and have successfully delivered similar complex SOC and SIEM engagements in the past. Therefore, bidder capability should ideally be evaluated based on demonstrated technical expertise, project experience, and delivery maturity rather than being narrowly constrained by partnership structure. In the interest of promoting wider participation, ensuring fair competition, and enabling the customer to receive the most technically and commercially optimal solution, we respectfully request the tender committee to consider revising this clause accordingly.	Bidder can have partnerships with multiple SIEM OEMs but can bid with SIEM solution of any one OEM only. The bidder must have a direct partnership with the supplier of the SIEM tool.
55				**Clarification on Contractual Terms,Definitive Agreements and Post-Bid Negotiation:-** Based on our review of the RFP, we note that only a few contractual clauses have been included, and some contractual terms are missing. We understand that, upon award of the bid, the Parties will enter into good faith negotiations to finalize and execute one or more definitive agreements, including but not limited to a Service Agreement, which will comprehensively govern the respective rights, obligations, liabilities, and risk allocation between the Parties. Kindly confirm if our understanding is correct.	The contract will be executed in accordance with the terms and conditions outlined in the RFP.

Response to Prebid Queries					
RFP Ref. No.		CPCM-03/2026-27 Date: 09-Apr-2026 GEM Bid No. GEM/2026/B/7427591			
RFP Name		Request for Proposal (RFP) FOR SELECTION OF SERVICE PROVIDER FOR IMPLEMENTATION & SUPPORT FOR SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT) PLATFORM AND MANAGED DETECTION & RESPONSE SERVICES (MDR)			
Sr. No.	Page No.	RFP Clause	Clause Description	Query	StockHolding Remarks
56				**We recommend to incorporate a new clause under the RFP, which shall be mutually beneficial and significant in the context of business engagements :-** **Non-Solicitation:-** During the Term of this definitive Agreement and for a period of one year thereafter, neither Party shall (either directly or indirectly through a third party) solicit to employ, cause to be solicited for the purpose of employment to any employee/s (including the employees who have been exposed or introduced to other Party during initial discussion between Parties or engaged to provide/perform the services under any definitive agreement entered between Parties) of the other Party or aid any third person to do so, without the specific written consent of the other Party. The said restriction shall also apply to each Party's affiliates, agents, vendors, contractors, and any third parties with whom such Party has a relationship (collectively, ""Representatives""). Parties agree that Representatives are equally restricted from poaching or soliciting or inducing any employees of other Party to leave their employment or engagement with such other Party	No Change
57				**It is recommended to include the below clause under the RFP:-** **Limitation of Liability:-** Notwithstanding anything to the contrary contained in this Agreement, the total aggregate liability of the Successful Bidder, whether arising in contract, tort (including negligence), strict liability or otherwise, shall not exceed the total fees/contract value paid or payable to the Successful Bidder under this Agreement. In no event shall the Successful Bidder be liable for any indirect, incidental, consequential, special, or punitive damages, including but not limited to loss of profits, loss of business, loss of data, or business interruption, even if advised of the possibility of such damages. The foregoing limitation shall not apply to (i) liability arising from fraud, gross negligence, or willful misconduct, or (ii) breach of confidentiality and data protection obligations, to the extent such exclusion is not permitted under applicable law.	No Change
58				**It is recommended to include the below clause under the Termination section as follows:-** **Termination by the bidder for breach:-** In the event Bank materially breaches this definitive Agreement or any statement of work, which breach is not cured within thirty (30) days after written notice specifying the breach is given to the Bank, the bidder may terminate this definitive Agreement or any portion thereof or the applicable statement of work by giving written notice to the Bank.	No Change

Response to Prebid Queries					
RFP Ref. No.		**CPCM-03/2026-27 Date: 09-Apr-2026 GEM Bid No. GEM/2026/B/7427591**			
RFP Name		**Request for Proposal (RFP) FOR SELECTION OF SERVICE PROVIDER FOR IMPLEMENTATION & SUPPORT FOR SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT) PLATFORM AND MANAGED DETECTION & RESPONSE SERVICES (MDR)**			
Sr. No.	**Page No.**	**RFP Clause**	**Clause Description**	**Query**	**StockHolding Remarks**
59	31	Indemnify	Indemnify The Bidder should hereby indemnify, protect and save StockHolding against all claims, losses, costs, damages, expenses, action suits and other proceedings, resulting from infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all the equipment offered by the Bidder. Any publicity by Bidder in which name of StockHolding is used should be done only with the explicit permission of StockHolding.	**We Propose to add:-** **Indemnify** The Bidder and the Contractor should hereby indemnify, protect and save each other against all claims, losses, costs, damages, expenses, action suits and other proceedings, resulting from infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all the equipment offered by the Bidder. Any publicity by Bidder and contractor in which name of each other is used should be done only with the explicit permission of one another.	No Change
60	9	Eligibility Criteria	4. The bidder must have executed a minimum of three (03) projects related to SIEM and MDR services in India during the last five (05) years as of the RFP date, with at least one (01) deployment handling not less than 2000 EPS (Events Per Second) or a minimum integration of 1000 devices with the deployed SIEM-MDR solution. Note: Bidder to submit the experience of proposed SIEM and MDR tool only for this RFP.	•Please change to Bidder /OEM •Bidder project execution limited to 1 customer with 1000 EPS	No Change
61	40	Incident Management Tool	20. The principal goal of the incident management process is to identify anomalous activities in the environment, contain those events and restore normal service operation as quickly as possible and minimize adverse impact on business operations, thus facilitating continued service quality and availability.	The containments of events & restore normal service operations are such capabilities typically require orchestration and automated response functionality through SOAR. "Kindly confirm if there is any requirement of SOAR solution as well."	**Clarification:** No SOAR platform in place and hence not to be considered in the scope of work
62	40	Incident Management Tool	23 .Bidder should also provide a detailed process for managing incidents - describing each phases of the process – prepare, identify, contain, eradicate/remediate, recover and learn from the incidents responded to.	The capabilities such as "contain, eradicate/remediate, recover" belong to SOAR, Kinldy confirm if there is any requirement for SOAR solution.	**Clarification:** No SOAR platform in place and hence not to be considered in the scope of work
63	40	Managed Detection and Response Services	30. Raising remediation tickets to pre-defined users withrecommendations and/or response playbooks	Features such as "response playbooks" belong to SOAR, Kindly confirm if there is any requirement of SOAR solution.	**Clarification:** No SOAR platform in place and hence not to be considered in the scope of work
64	41	Brief description of how operations are performed post Implementation	38. As a part of the Standard MDR offering, Service Provider should detect, investigate and contain threats. Post that, they will send out tickets to StockHolding's SOC team for mitigation and response actions within our network. They will also provide playbooks and knowledge base to help us resolve these tickets. StockHolding's SOC team can reach back to them for query resolution but such support is provided on best effort basis.	"To contain threat", is a feature of SOAR solution. Kindly confirm if there is any requirement of SOAR solution.	**Clarification:** No SOAR platform in place and hence not to be considered in the scope of work
65	39	Solution Implementation	10. The SIEM should be able to collect logs from the devices/applications/databases etc. mentioned by StockHolding as per the SOW including the solutions deployed as part of this RFP. It should be able to collect the logs from devices from geographically dispersed locations i.e. DC, DR and branch offices, etc.	Kindly mention the number of locations of DC, DR, NDR & branch offices, whose logs needs to be monitored.	**Clarification:** All logs are centrally pushed to log aggregator server. The bidder has to ensure that the logs are ingested in the SIEM platform which shall be hosted at the Vendor's end. Log Aggregator server is at centrale level. Logs across branches are available in the central log server
66			Kindly confirm whether DC,DR & NDR are in High Availability or not.		**Clarification:** Please refer sections pertaining to SLA and Penalty and Deploy the SIEM-MDR Solution accordingly. Bidder has to ensure the SIEM platform is available as per SLA's and take the necessary steps to ensure uptime availability. It is the choice of bidder to have DR or HA or any other model to upkeep the uptime availability

Response to Prebid Queries					
RFP Ref. No.		**CPCM-03/2026-27 Date: 09-Apr-2026 GEM Bid No. GEM/2026/B/7427591**			
RFP Name		**Request for Proposal (RFP) FOR SELECTION OF SERVICE PROVIDER FOR IMPLEMENTATION & SUPPORT FOR SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT) PLATFORM AND MANAGED DETECTION & RESPONSE SERVICES (MDR)**			
Sr. No.	**Page No.**	**RFP Clause**	**Clause Description**	**Query**	**StockHolding Remarks**
67	36	ANNEXURE – 3 – Technical Criteria & Compliance	4. OEM solution must be positioned in the respective Leader's quadrant/category of the latest IDC MarketScape or Gartner Magic Quadrant, or Forrester Wave reports for proposed SIEM Solution Presence of OEM Solution in Leader's quadrant/category – 10 Marks	Kindly Requesting to give Exemption or Waive Off for this Clause, This will help more Make In India startups to come forward and particpate in this opportunity With Reference to Public Procurement (Preference to Make In India) Order 2019 from MeitY Point No.8:-In any procurement process, the procuring entity shall not specify any mandatory qualification criteria, any eligibility specifications or certification(s) issued by any foreign testing/security lab(s)/analyst reviews which restricts eligibility of Indian cyber security products as defined in this order.	No change This is not a mandatory requirement for participation but a part of technical scoring criteria.
68	36	ANNEXURE – 3 – Technical Criteria & Compliance	Projects for implementation of SIEM and MDR services with at least 1 deployment not less than 2000 EPS (Events per Second) each during last 05 (five) years in India Note: Bidder to submit the experience of proposed SIEM and MDR tool only for this RFP. • 1-3 Projects – 10 Marks • 4-5 Projects – 12 Marks • More than 5 Projects – 15 Mark	This clause is restricting multiple Bidders and OEMs of different make and models to participate in the tender because in each and every bid or tender, the products quoted regularly will change and the bidder always looks at the best commercial models quoted by the OEM. So it will be difficult for bidders as well as OEMs to participate in this opportunity. Kindly amend this clause to " **Note: Bidder to submit the relevant experience of SIEM and MDR**" that will help multiple Bidders and OEMs to participate in this opportunity and it helps the customer also to get the best of the products available in the market to cater the requirement.	No Change
69	34	ANNEXURE - 2 – Eligibility Criteria	The bidder must have executed a minimum of three (03) projects related to SIEM and MDR services in India during the last five (05) years as of the RFP date, with at least one (01) deployment handling not less than 2000 EPS (Events Per Second) or a minimum integration of 1000 devices with the deployed SIEM-MDR solution. Note: Bidder to submit the experience of proposed SIEM and MDR tool only for this RFP.	Please revised this Clause as a The **bidder/OEM** must have executed a minimum of three (03) projects related to SIEM and MDR services in India during the last five (05) years as of the RFP date, with at least one (01) deployment handling not less than 2000 EPS (Events Per Second) or a minimum integration of 1000 devices with the deployed SIEM-MDR solution. Note: Bidder to submit the experience of proposed SIEM and MDR tool only for this RFP.	No Change
70	36	ANNEXURE – 3 – Technical Criteria & Compliance	Projects for implementation of SIEM and MDR services with at least 1 deployment not less than 2000 EPS (Events per Second) or a minimum integration of 1000 devices with the deployed SIEM-MDR solution each during last 05 (five) years in India Note: Bidder to submit the relevant experience only of the SIEM and MDR tool proposed for this RFP. • 1-3 Projects – 10 Marks • 4-5 Projects – 12 Marks • More than 5 Projects – 15 Marks	Please revised this Clause as a Projects for implementation of EDR/XDR services with a minimum of 1000 devices each during last 05 (five) years in India • 1-3 Projects – 10 Marks • 4-5 Projects – 12 Marks • More than 5 Projects – 15 Marks	No Change
71	36	ANNEXURE – 3 – Technical Criteria & Compliance	Projects of SIEM and MDR services implementation in BFSI Sector in India during last 05 (five) years in India • 1-3 Projects – 5 Marks • 4-5 Projects – 7 Marks • More than 5 Projects – 10 Marks	Please revised this Clause as a Projects for implementation of EDR/XDR services with a minimum of 1000 devices each during last 05 (five) years in India • 1-3 Projects – 10 Marks • 4-5 Projects – 12 Marks • More than 5 Projects – 15 Marks	No Change
72	36	ANNEXURE – 3 – Technical Criteria & Compliance	Customer reference for proposed SIEM-MDR Solution during the last 5 years as on RFP date 3 Customer reference Feedback from existing customer 2 = Average, 3 = Good, 4 = Excellent	Please revised this Clause as a Customer reference for EDR/XDR Solution during the last 5 years as on RFP date 3 Customer reference Feedback from existing customer 2 = Average, 3 = Good, 4 = Excellent	No Change

Response to Prebid Queries					
RFP Ref. No.		**CPCM-03/2026-27 Date: 09-Apr-2026 GEM Bid No. GEM/2026/B/7427591**			
RFP Name		**Request for Proposal (RFP) FOR SELECTION OF SERVICE PROVIDER FOR IMPLEMENTATION & SUPPORT FOR SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT) PLATFORM AND MANAGED DETECTION & RESPONSE SERVICES (MDR)**			
Sr. No.	**Page No.**	**RFP Clause**	**Clause Description**	**Query**	**StockHolding Remarks**
73				EPS cap to be considered is 2000 or 5000 as both will have price difference of 100%	Minimum EPS cap to be considered is 2000. Vendor can provide rate card for the bucket size for the incremental EPS